

6. Ataques remotos y locales

Proceso

67%



Índice

- 6.1 Clasificación de los ataques
- 6.2 Ataques remotos en UNIX
- 6.3 Ataques remotos sobre servicios inseguros en UNIX
- 6.4 Ataques locales en UNIX
- 6.5 ¿Qué hacer si recibimos un ataque?



6.1. CLASIFICACIÓN DE LOS ATAQUES



Según la naturaleza de los ataques que se pueden realizar contra una red informática, estos pueden ser divididos principalmente entre:

Activos

Pasivos

¿Qué distingue a cada uno de ellos?

¡Vamos a verlo! Haz clic sobre el primer botón

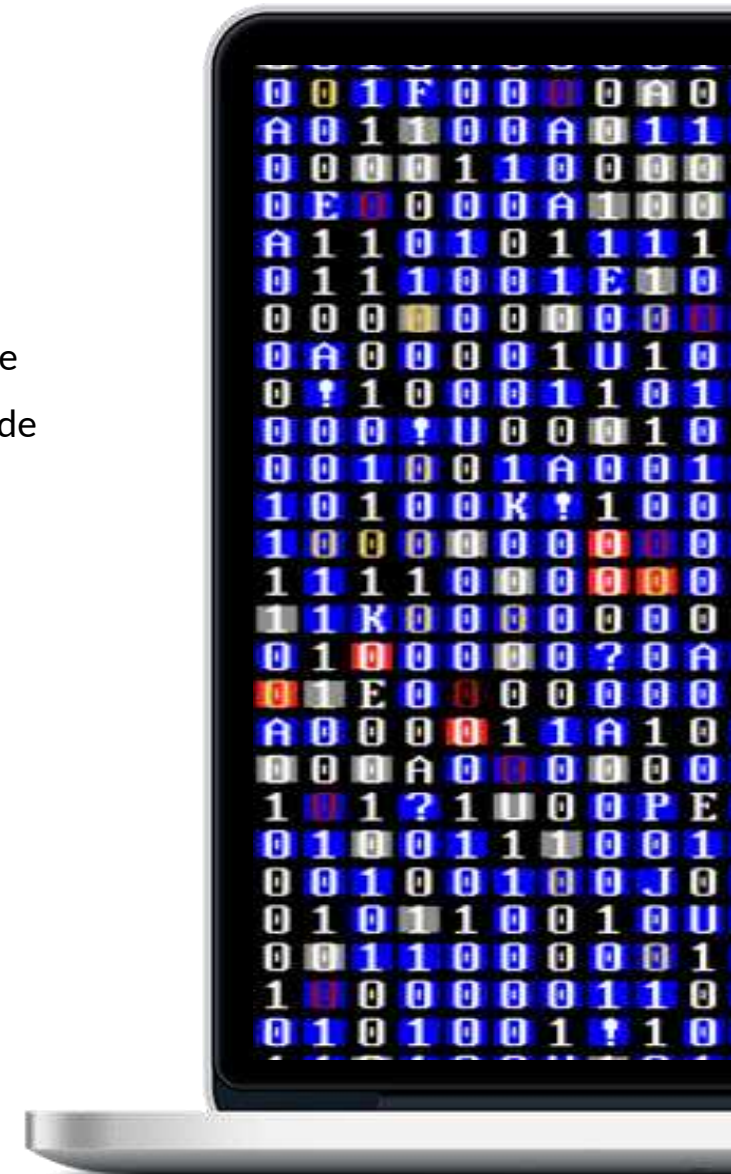
Los ataques activos

Son aquellos que **no solamente acceden a los datos, sino que realizan algún tipo de modificación en ellos**. Es por eso que influyen activamente en la información, creando cambios y, por lo tanto, una nueva corriente de datos.

Algunas de las **tácticas** más utilizadas son:



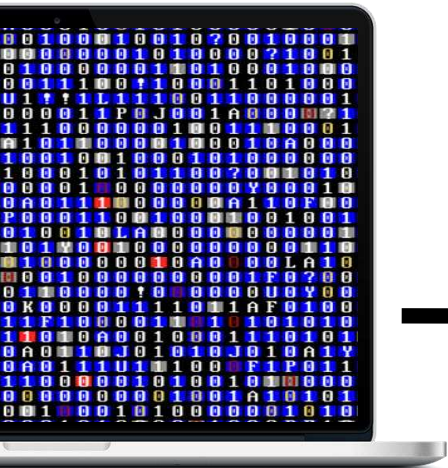
Haz clic aquí



Los ataques activos

Son aquellos que **no solamente acceden a los datos, sino que realizan algún tipo de modificación en ellos**. Es por eso que influyen activamente en la información, creando cambios y, por lo tanto, una nueva corriente de datos. Algunas de las **tácticas** más utilizadas son:

[Haz clic sobre los enunciados](#)



Reactuación

Se utilizan mensajes legítimos para repetirlos de forma que se logren resultados acordes al interés del atacante.

Alteración de mensajes

Se trata de coger un texto legal y modificarlo de forma que el mensaje final sea muy distinto al principal.

Cambios en el servicio

Modifica el uso normal del servicio, impidiendo su uso en determinados sectores o hacia entidades en concreto con el objetivo de extraer un beneficio de esta variación.

Suplantación de identidad

En este tipo de ataque activo, el usuario se camufla y se hace pasar por otra entidad para extraer beneficios de ella, como por ejemplo contraseñas.

Los ataques pasivos

Son los ataques en los que el atacante tan solo accede a los datos, sin realizar ningún tipo de modificación en ellos. Por esto, se puede decir que no influyen de forma activa sobre la información, sino que tratan de **interceptar los datos y analizar el tráfico**.

¿Qué se consigue con esta técnica?

- Conocer de dónde viene y a quién va dirigida la comunicación.
- Controlar el tráfico y las horas de intercambio, para conocer a fondo la actividad.

De esta forma, pueden acceder a información acerca de los datos que se manejan sin necesidad de tener que influir en ellos. Se convierten así en ataques pasivos muy difíciles de detectar por la ausencia de alteración.



¿Quién puede llevar a **cabo todos estos ataques?**

Vamos a ver los principales sujetos que nos podemos encontrar, aunque cabe destacar que cada uno de los “atacantes pasivos” se pueden convertir en “atacantes activos” en determinados contextos o bajo distintas motivaciones:

¿Quién puede llevar a cabo
todos estos ataques?



Crackers

I

Se trata de los atacantes más frecuentes en UNIX. Aprovechan los sistemas de seguridad media para acceder a los equipos con fines que pueden ser desde protesta hasta simple diversión. Suelen ser **atacantes pasivos**.



Siguiente

¿Quién puede llevar a cabo
todos estos ataques?

Atrás



Curiosos



Es otro de los grupos que más accede a UNIX a la hora de realizar sus ataques. Aunque sus objetivos no suelen ser la destrucción de los sistemas, lo cierto es que sus acciones no acarrearán nada positivo. Suelen ser **atacantes pasivos**.



Siguiente

¿Quién puede llevar a cabo todos estos ataques?

Atrás



Personal

I

Cuando el ataque es intencionado, juegan con la ventaja de ser presupuestos como gente de confianza. Sin embargo, la mayor parte de las veces se trata de ataques intencionados o accidentes. Pueden ser **tanto atacantes activos como pasivos**, dependiendo de si se trata de un acto intencionado o de un contratiempo.



Siguiente

¿Quién puede llevar a cabo
todos estos ataques?

Atrás



Ex-empleados

|

Suelen ser personas que no están contentas con la organización y que utilizan toda la información que conocen de ella para atacarla. Son **atacantes activos**.



Siguiente

¿Quién puede llevar a cabo
todos estos ataques?

Atrás



Terroristas



Atacan al sistema con el único objetivo de
causarle daño y las motivaciones pueden
ser desde religiosas hasta políticas. Son
atacantes activos.



Siguiente

¿Quién puede llevar a cabo
todos estos ataques?

Atrás



Intrusos remunerados

I

Es el grupo menos frecuente, pero también el más peligroso. Son personas con mucha experiencia y con un gran respaldo económico y de poder a sus espaldas, capaces de conseguir con facilidad los objetivos que se proponen. Son **atacantes pasivos** si tienen un objetivo distinto a nuestra red y **atacantes activos** en caso de que estemos en su punto de mira.



6.2. ATAQUES REMOTOS EN UNIX

Ataques remotos

Los ataques remotos son aquellos que **se llevan a cabo por usuarios a través de redes y ordenadores para atentar contra la seguridad de los mismos a través de la red**. Buscan vulnerabilidades en el sistema (como fallos de seguridad en el software) para poder acceder a través de ellas y entrar al equipo informático.

Objetivo principal

Su **objetivo principal es conseguir información acerca de la empresa en cuestión** para utilizarla en su propio beneficio y lo suelen hacer a través de herramientas, como los programas malware.



Se trata, por lo tanto, de aquellos ataques en los que el agresor realiza sus incursiones por medio de redes de telecomunicaciones, como puede ser Internet, de entre los que destacan los siguientes:

Phishing

Redes Sociales

Vishing



Redes Sociales

Vishing

Phishing

Seguramente en algún momento, mientras navegabas por la red, te has encontrado las típicas “**páginas falsas**” que **simulan ser las originales**, con el objetivo principal de conseguir toda la información posible y utilizarla para fines ilegales. Una particularidad del phishing es que puede acudir a técnicas basadas en el sentimentalismo para jugar con la víctima, creándole una necesidad de “ayudar”.



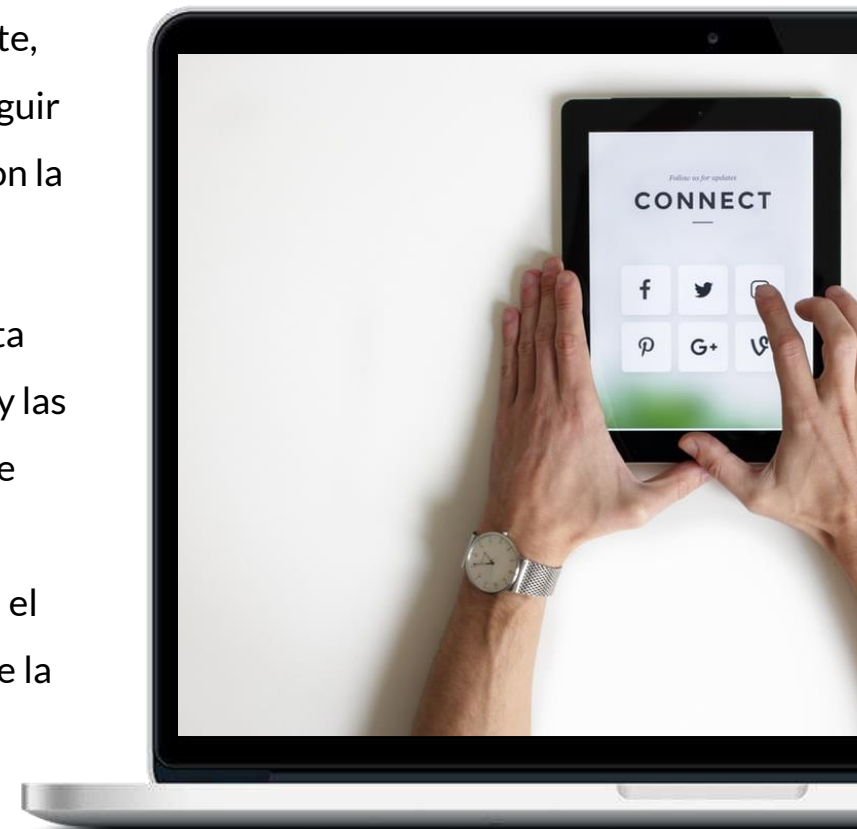
Phishing

Redes Sociales

Hoy en día una gran parte de nuestra información privada se encuentra (de unas maneras u otras) reflejada en nuestras redes sociales. Es por ello que actualmente se trata de una técnica muy recurrente, que tiene como principales propósitos el de conseguir la información de la víctima y crear una relación con la misma, para utilizarlo en beneficio propio.

Pero, en contra de lo que podría parecer, no se trata solo de un problema personal; y es que a día de hoy las empresas también tienen redes sociales, por lo que sus empleados necesitarán llevar cuidado con su información y con la de la empresa para evitar que el problema sea mayor y repercuta en la seguridad de la misma.

Vishing

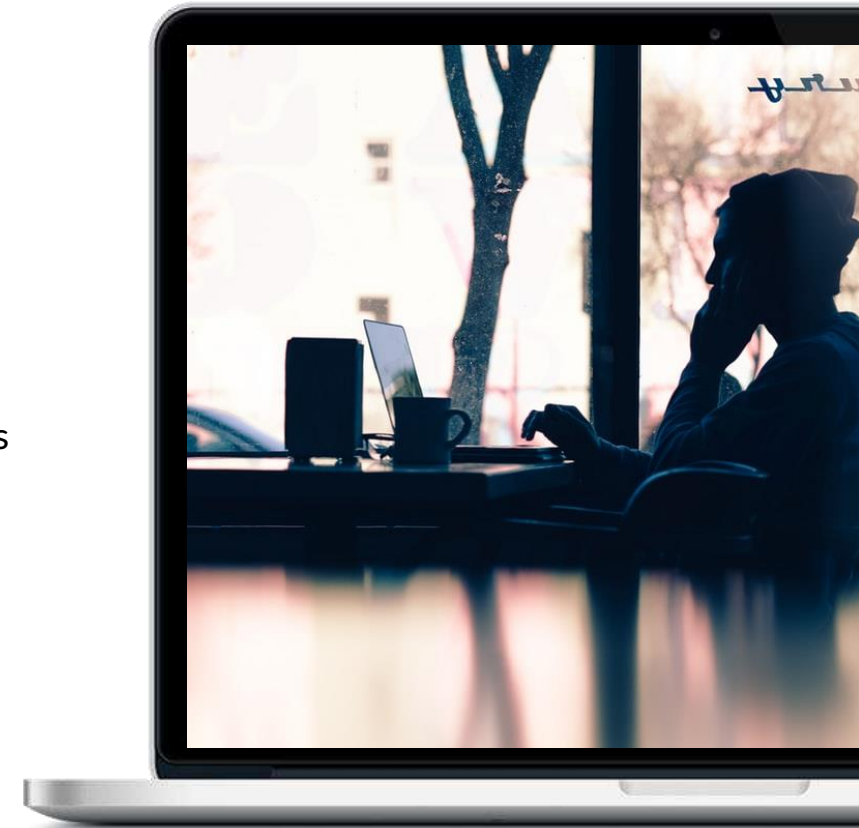


Phishing

Redes Sociales

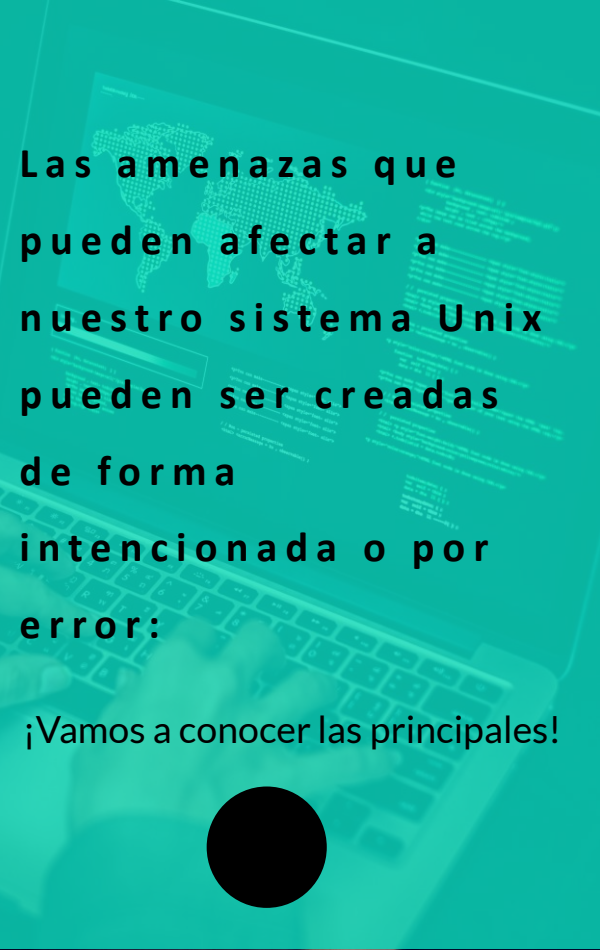
Vishing

Se trata de una técnica de ataque a la seguridad de la información **a través de llamadas de teléfono**. A través de diversos engaños se intenta que la persona revele datos muy importantes y privados. Es muy similar al Phishing, pero utilizan las tecnologías de voz para conseguir sus objetivos.





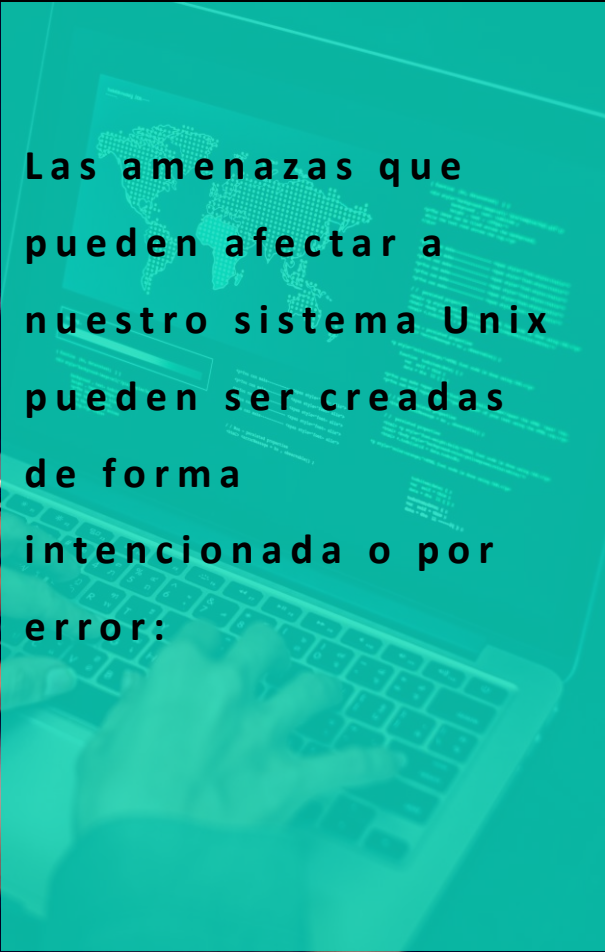
6.3. ATAQUES REMOTOS SOBRE SERVICIOS INSEGUROS EN UNIX



**Las amenazas que
pueden afectar a
nuestro sistema Unix
pueden ser creadas
de forma
intencionada o por
error:**

¡Vamos a conocer las principales!





Las amenazas que pueden afectar a nuestro sistema Unix pueden ser creadas de forma intencionada o por error:

Software incorrecto

Uno de los principales problemas con los que se encuentran los sistemas Unix, ya que provienen de errores cometidos de forma involuntaria por los programadores en el momento de su puesta en marcha. Estos errores de programación son reconocidos bajo el término “bugs”.

Herramientas de seguridad

De la misma forma que sirven para encontrar los errores o amenazas y repararlas, también pueden ser utilizadas para el efecto contrario: encontrar vulnerabilidades para actuar contra el sistema.

Puertas traseras

Atajos puestos en marcha por los programadores para conseguir más velocidad a la hora de detectar fallos. Si algún atacante encuentra estas puertas traseras, se puede convertir en un gran problema, ya que este tendrá acceso a todos los datos.

Virus

Su función principal es la de ir insertándose e infectando los archivos y ficheros. Sin embargo, lo cierto es que en Unix no constituyen una amenaza tan grande como en otros sistemas operativos, ya que lo más probable es que un atacante tenga más fácil acceder a otros mecanismos.

Gusanos

Se propagan en cuestión de segundos, por lo que son capaces de controlar redes enormes de forma sumamente fácil. Es por ello que se trata de una gran amenaza para los dispositivos Unix.

Caballos de Troya

Programa que contiene unas normas o instrucciones distintas a las que muestra o aparenta. Una vez dentro del sistema, ejecuta las funciones ocultas sin que el usuario pueda hacer nada.



6.4. ATAQUES LOCALES EN UNIX

Ataques locales

Se trata de aquellos ataques en los que el agresor, sin tener que recurrir a ningún tipo de conexión, acude físicamente al lugar en cuestión a realizar el ataque. Existen varios tipos de ataques locales, de entre los que destacamos algunas técnicas como:

- Trashing o Dumpster Diving
- Shoulder Surfing
- Pretexting
- Tailgating
- Distracción
- Aprovechar los errores de seguridad





Shoulder Surfing

Pretexting

Tailgating

Distracción

Aprovechar los errores de seguridad

Trashing o Dumpster Diving

Se trata de una técnica muy recurrida actualmente, y es que **hay mucha información entre las cosas que arrojam**os a **nuestra basura** sin que nosotros nos demos ni cuenta. Usuarios, contraseñas, fechas, números de cuenta, emails... muchos datos que pueden ayudar al atacante a recabar información sobre la víctima.





Trashing o Dumpster Diving



Pretexting - impersonate



Tailgating



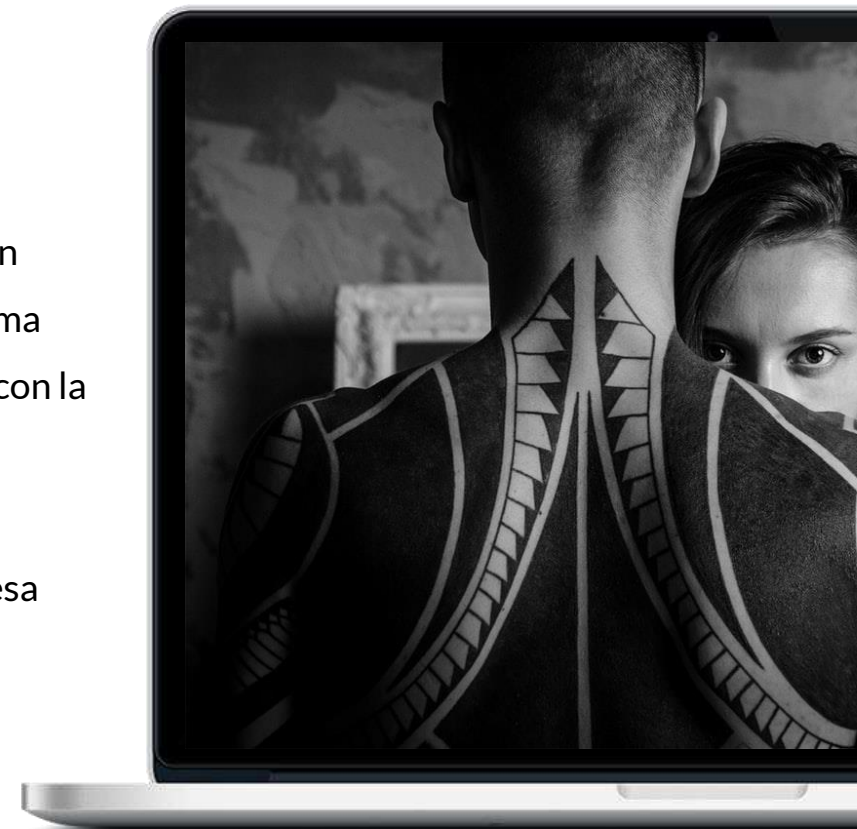
Distracción



Aprovechar los errores de seguridad

Shoulder Surfing

Su función puede parecer tan básica como “mirar por encima del hombro” a las personas, con la intención de observar qué contraseñas o cuentas introducen y poder utilizar esa información para su propio beneficio.





Trashing o Dumpster Diving



Shoulder Surfing



Tailgating



Distracción



Aprovechar los errores de seguridad

Pretexting - impersonate

Se trata de dos técnicas que se retroalimentan. Ya que, mientras que el **impersonate** sirve para que el atacante pueda hacerse pasar por el empleado, y con el **pretexting** este crea una justificación para intervenir en su actividad y acceder fácilmente a los datos que maneja.



Trashing o Dumpster Diving

Shoulder Surfing

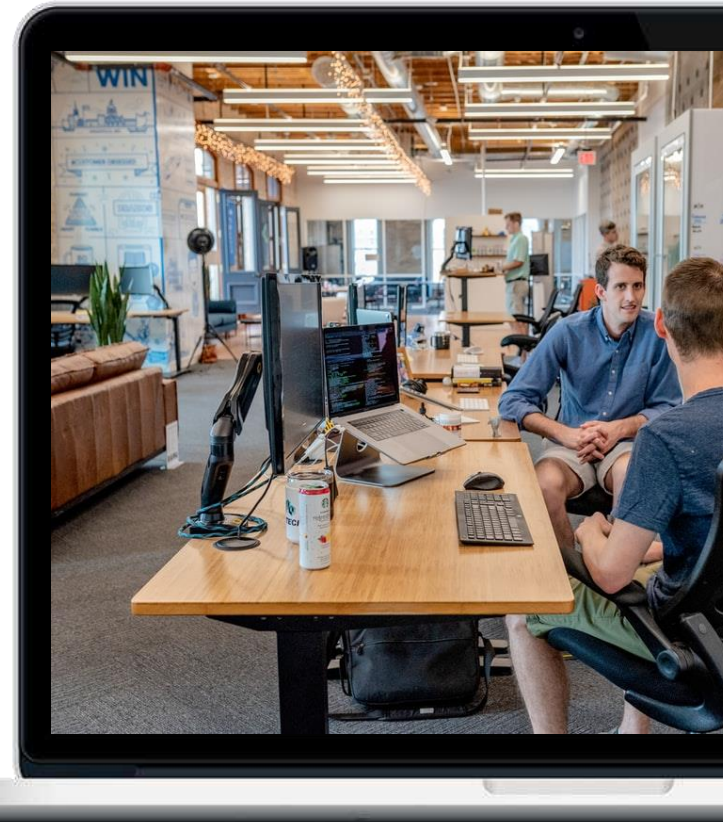
Pretexting

Tailgating

A diferencia del caso del pretexting, el tailgating utiliza sus tácticas para aprovecharse de la buena fe de los trabajadores, creando una confianza para acceder a datos e información de la empresa sin levantar sospechas.

Distracción

Aprovechar los errores de seguridad





Trashing o Dumpster Diving



Shoulder Surfing



Pretexting



Tailgating



Aprovechar los errores de seguridad

Distracción

Esta táctica se basa en crear en el trabajador un foco de atención distinto al que debería tener. De esta forma, el atacante podrá acceder a lo que el trabajador ha “dejado de lado” y recopilar información y datos.



● Trashing o Dumpster Diving

● Shoulder Surfing

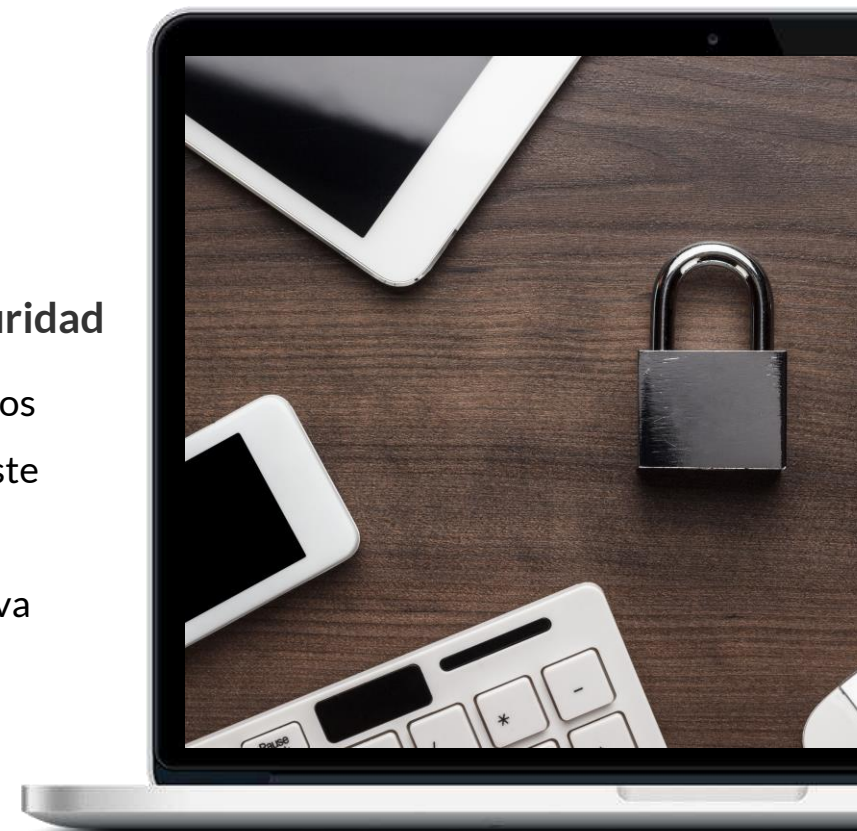
● Pretexting

● Tailgating

● Distracción

Aprovechar los errores de seguridad

Se trata sin duda alguna de uno de los métodos más utilizados, ya que existe un gran número de empresas actualmente que no prestan excesiva atención a la seguridad de sus controles.





6.5. ¿QUÉ HACER SI RECIBIMOS UN ATAQUE?

En general los usuarios de Unix en entornos del día a día son personas muy poco formadas en el manejo del sistema operativo y, mucho menos, en lo que a seguridad informática se refiere. La única preocupación es que sus datos estén listos cuando los requieren, de la forma más fácil y rápida posible.

El responsable de seguridad ha de concienciar a todas estas personas de la necesidad de la seguridad para que el entorno de trabajo funcione. Además de esto último para conseguir un sistema fiable y evitar los ataques es necesaria la **formación** de los mismos.





¡Enhorabuena!

Has conseguido superar la sexta unidad. Continúa con el curso para... ¡Ser el mejor en gestión de la seguridad informática en tu empresa!